An Intelligent Threat Prevention Framework with Heterogeneous Information

Ma, W., & Liu, W. (2014). An Intelligent Threat Prevention Framework with Heterogeneous Information. In *21Sst European Conference on Artificial Intelligence (ECAI 2014)* (pp. 1061-1062). (Frontiers in Artificial Intelligence and Applications). https://doi.org/10.3233/978-1-61499-419-0-1061

Published in:
21Sst European Conference on Artificial Intelligence (ECAI 2014)

Document Version:
Publisher's PDF, also known as Version of record

ECAI 2014
T. Schaub et al. (Eds.)

doi:10.3233/978-1-61499-419-0-1061

An Intelligent Threat Prevention Framework with Heterogeneous Information

Wenjun Ma [1] and **Weiru Liu** [1]

Abstract. Three issues usually are associated with threat prevention intelligent surveillance systems. First, the fusion and interpretation of large scale incomplete heterogeneous information; second, the demand of effectively predicting suspects' intention and ranking the potential threats posed by each suspect; third, strategies of allocating limited security resources (e.g., the dispatch of security team) to prevent a suspect's further actions towards critical assets. However, in the literature, these three issues are seldomly considered together in a sensor network based intelligent surveillance framework. To address this problem, in this paper, we propose a multi-level decision support framework for in-time reaction in intelligent surveillance. More specifically, based on a multi-criteria event modeling framework, we design a method to predict the most plausible intention of a suspect. Following this, a decision support model is proposed to rank each suspect based on their threat severity and to determine resource allocation strategies. Finally, formal properties are discussed to justify our framework.

1 Introduction

The demand for intelligent surveillance systems is growing rapidly due to the increased threats to the public and society. In order to prevent threats, in many real-world applications, a security system should not only predict the intentions of suspects and rank the potential threats, but also allocate the security resources to prevent the most plausible and dangerous threat. However, given that most of current surveillance frameworks in this domain only focus on some of the three related issues we mentioned in abstract, they are not well suited to model and reason with heterogeneous information used in a complex security surveillance situation.

In this paper, we develop a novel intelligent surveillance framework coupling lower-level event detection from multiple sources with high-level prediction and decision making. The lower-level is to process heterogeneous sensor information to derive events with rich semantic information such as critical characteristics of subjects being monitored. The high-level is responsible for analyzing the intentions of suspects, prioritizing threats posed by different suspects, and selecting optimal strategies based on limited security resources. Figure 1 illustrates the architecture of our framework.

Our main contributions are as follows: (i) we propose a framework that is able to fuse heterogeneous sensor information under uncertainty, and make use of fusion results to support decisions; (ii) we define a method to analyze the intention of a suspect, which considers the criteria weights, the priority for each state of each criterion, and the uncertain information obtained by classification algorithms;

[1] School of EEECS, Queen's University Belfast, {w.ma,w.liu}@qub.ac.uk

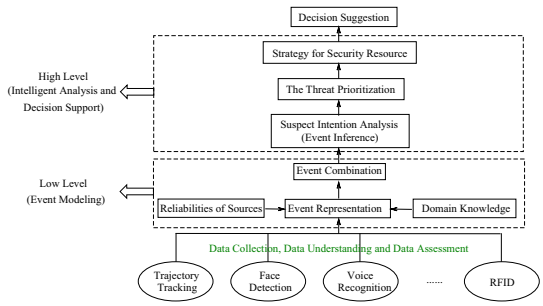

Figure 1. Multi-Levels Surveillance Framework Architecture

(iii) our framework can select optimal strategies for decision support under limited security resources.

2 Suspect Intention Recognition

The lower-level of our surveillance system can be constructed by the multi-criteria event modeling framework in [2] to represent events from multiple sources with uncertain and incomplete information. Following this, we consider the second key issue about how to differentiate normal intentions from malevolent ones. To achieve this, we associate malevolent intentions with the concept of suspect type in security game framework [5]: such as *Robber, Bomber, Gunman*, etc. That is, if a suspect is a *Robber*, his intention is to rob someone.

Such a suspect intention recognition problem can be addressed by extending the method in [3] to include event inference as follows:

Step 1: Determine intentions (types) in frame Θ and related criteria for a suspect based on the observed events.

Step 2: Create inference rules to correlate events for different behaviors, and dynamically generate the mass functions over the frames for the rules of different behaviors $\{\mathsf{satisfied}\ \mathsf{R}_1, \ldots, \mathsf{satisfied}\ \mathsf{R}_n, \mathsf{satisfied}\ \mathsf{NoRules}\}$ *(where* $\mathsf{satisfied}\ \mathsf{R}_1$ *means only R_1 (no other rules) is satisfied) based on events observed under uncertainty (events that are part of rule conditions).*

Step 3: Construct the preference matrix, mass function m_c, utility function u_c and normalized weight $(\omega_i / \sum \omega_i)$ for each criterion.

Step 4: Determine the mass function $m_{v_c^i,t}$ about the suspect's types for each criterion's state by DS/AHP method [1].

Step 5: Obtain the set of mass functions $\{m_{c,t}(x)\}$ about a suspect's type for each criterion. And

$$m_{c,t}(x) = \sum_{v_c^i \in \Omega_c} \sum_{V \bigcap v_c^i \neq \emptyset} \frac{u(v_c^i)}{\sum\{u(v_c^j) \mid v_c^j \in V\}} m_c(V) m_{v_c^i,t}(x).$$

Step 6: Obtain the overall mass function $m_t(x)$ of suspect's types by combining $m_{c,t}$ for each criterion with Dempster's combine rule. Thus, $m_t(x)$ implies a suspect's possible intention.

Moreover, to avoid overloading a security system, some predefined thresholds are used to eliminate subjects that will not cause security concerns, and concentrate only on highly suspicious ones. The reason of setting these thresholds is that: the criteria with lower weights or the criterion's states with lower level of potential threats always show that the person is normal in our method. Thus, a criterion with a higher weight will be triggered to predict the suspect's type, if the mass values of some states with high potential threat levels are greater than a required threshold. Hence, only the subjects with a high-weight triggered criterion are remained for intention analysis.

3 Decision Support with Limited Resources

Decision support with limited resources requires information such as the priority of suspects and the locations of resources dispatched.

First, we consider the priority of suspects. After detecting the suspects' intention and defining the level of potential threat for each possible intention $t_i \in \Theta$ by a utility function $u : \Theta \longrightarrow R$, where R is the real number set, we can obtain the point-valued potential threat degree w.r.t. each suspect and rank the priorities of the suspects by the method in [2]. Moreover, assigning the available security resources can be achieved by the following method: first, determine the maximum available security resources and the maximum required resources for each suspect based on his potential attack targets. Second, set the ordering of suspects based on their potential threat degrees. Third, set a threshold value k to distinguish less severe threats from significant ones. Forth, eliminate the suspects whose potential threat degrees are less than k. Fifth, assign the security resources one by one according to the priorities of the remained suspects in the order of threat levels (from high to low) until all the resources are allocated or all suspects being assigned maximum required resources.

Also, suspects with different intentions might have different preferences over the choices of their next moves. Thus, in order to find out the optimal strategy to dispatch security resources, the system should consider the ambiguity of suspect's type (intention), the available security resources, and the importance of a potential attack target for a given suspect. Here, since it is unrealistic to assume a suspect knows a defender's belief about his type (intention), a defender's selected strategy and the amounts of available resources in the real-time surveillance environment, current solution concepts in security games are not well-suited to model ambiguous threat prevention games. Based on the *minimax regret* principle [4] and the decision rule under ambiguity in [2], the whole process of finding the optimal strategy of defender can be solved by a Mixed-Integer Quadratic Program as follows (where $V = \min_{q_l} \max_{a_h} (\max_{b_k \in A_2} u_{2,t}(a_h, b_l) - \sum_{j=1}^{n} u_{2,t}(a_h, b_j) q_l^t)$ is the value of minimax regret mixed strategy of suspect type t):

$$
\begin{aligned}
\max \quad & \Sigma_{i=1}^{n} \Sigma_{j=1}^{n} \Sigma_{A \subseteq \Theta} \, p_i((1-\delta(k)) m_t(A) \min\{u_{1,t}(a_i, b_j) q_j^t \mid \\
& t \in A\} + \delta(k) m_t(A) \max\{u_{1,t}(a_i, b_j) q_j^t \mid t \in A\}) \\
\text{s.t.} \quad & \Sigma_{i=1}^{n} p_i = m, \Sigma_{j=1}^{n} q_j = 1 \\
& \forall a_h \in A_2, \ \max_{b_k \in A_2} u_{2,t}(a_h, b_k) - \Sigma_{j=1}^{n} u_{2,t}(a_h, b_j) q_j^t \leq V \\
& p_i \in \{0, 1\}, q_j \in [0, 1]
\end{aligned}
$$

Here for the threat prevention security resources allocation strategy of a defender (denoted by p_i for the assignment of m security resources to each pure strategy $a_i \in A_1$) and the possible attack target selection by each type of suspect (denote by q_j^t for the probabilities assignment of suspect type t to each pure strategy $b_j \in A_2$), the objective function represents the expected reward for the defender considering the mass distribution $m_t(A)$ over the suspect types (intentions) and the significant degree $\delta(k)$ for the related events. The first part of the first and the third constraints limit the strategies selected by the defender being a pure distribution over A_1 (that is, each p_i either exactly equal to one or exactly equal to zero). Note that we need to consider only the reward-maximizing pure strategies of defender, since for the given fixed mixed strategies of all suspect types, the defender faces a problem with fixed linear rewards after applying rule in [2]. If a mixed strategy is optimal for the defender, then so are all the pure strategies in support of that mixed strategy. Moreover, the second part of the first and the third constraints define the set of possible attack targets selection by a suspect of type t, where q_j^t is a probability distribution over the set of actions A_2. Finally, the second constraint ensures that each type of suspect will adopt the minimax regret strategy as his optimal strategy.

4 Properties

In fact, our framework satisfies some desirable properties that an intelligent surveillance system should have.

Property 1: The possible intention of a suspect is determined by the inference result of fusing all criteria information together.

Property 2: The higher weight a criterion has, the higher influence it has on the result of suspect intention recognition, *ceteris paribus*. And the higher preference ranking value is for a suspect's type in a state of a criterion, the more possible it becomes the most plausible intention of the suspect, *ceteris paribus*.

Property 3: If by a classification algorithm, a criterion is classified as a state with a certainty p, then the higher value of p, the more possible for the type with the highest preference ranking value in this state becomes the most plausible intention of the suspect, *ceteris paribus*. And the higher the level of potential threat for a given state v_i^c is, the more possible for the type with the highest preference ranking value in this state becomes the most plausible intention of the suspect, *ceteris paribus*.

Property 4: For decision under ambiguity, if the worst condition of a choice has a higher expect utility than the best condition of another, we should choose the former; if the significance degree of a choice is not less than that of another, and the worst and best conditions of this choice has a higher expect utility than those of another respectively, we should choose this choice; and for two expect utility intervals with the same center and one covers another, the significance degree will determine our choice.

5 Conclusion

This paper proposes an intelligence surveillance framework to handle three key issues in complex surveillance situations: event modeling, suspect intention recognition (event inference), decision support with limited security resources. First, we introduced a suspect's intention recognition method to predict the suspects' plausible intentions. After that, we proposed a mixed-integer quadratic program to determine the defender's optimal strategy. Furthermore, we stated some desirable properties of an intelligent surveillance system and proved that our framework satisfies these properties.

REFERENCES

[1] M. Beynon, 'DS/AHP method: A mathematical analysis, including an understanding of uncertainty', *Eur. J. of Op. Research.*, **140**(1), 148–164, (2002).

[2] W. Ma, W. Liu, J. Ma, and P. Miller, 'An extended event reasoning framework for decision support under uncertainty', in *IPMU 2014*. Montpellier, France, (2014).

[3] W. Ma, W. Liu, P. Miller, and X. Luo, 'A game-theoretic approach for threats detection and intervention in surveillance', in *AAMAS'14*. Paris, France, (2014).

[4] L. J. Savage, 'The theory of statistical decision', *J. of the Amer. Stat. Asso.*, **46**(253), 54–67, (1951).

[5] M. Tambe, *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*, Cambridge University Press, Cambridge, 2011.